UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/563,504	06/23/2006	Udo Doebrich	2003P05083WOUS	8240

22116 7590 04/28/2008

SIEMENS CORPORATION
INTELLECTUAL PROPERTY DEPARTMENT
170 WOOD AVENUE SOUTH
ISELIN, NJ 08830

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
04/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/563,504	DOEBRICH ET AL.	
	Examiner	Art Unit	
	Christian LaForgia	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *24,25,27-30,33-35,37 and 40-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *24,25,27-30,33-35,37 and 40-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 17 January 2008 has been noted and made of record.

2. Claims 24, 25, 27-30, 33-35, 37 and 40-49 have been presented for examination.

3. Claims 1-13, 26, 31, 32, 36, 38, and 39 have been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's arguments, see page 11, filed 17 January 2008, with respect to the 35 U.S.C. 112, 2nd paragraph rejection have been fully considered and are persuasive. The 35 U.S.C. 112, 2nd paragraph rejection of claims 24-44 has been withdrawn.

5. Applicant's arguments, see page 11, filed 17 January 2008, with respect to the 35 U.S.C. 101 rejection have been fully considered and are persuasive. The 35 U.S.C. 101 rejection of claim 39 has been withdrawn.

6. Applicant's arguments with respect to the prior art rejections of claims 24, 25, 27-30, 33-35, 37 and 40-49 have been considered but are moot in view of the new grounds of rejection set forth below.

Claim Objections

7. Claim 30 is objected to because of the following informalities: the third limitation states "transmitting the second random value tothe first user." For the sake of examination the Examiner will interpret the limitation as "transmitting the second random value to the first user." Appropriate correction is required.

8. Claim 37 is objected to because of the following informalities: it depends from a claim that has been cancelled. For the sake of examination the Examiner will construe claim 37 depending from claim 24. Appropriate correction is required.

9. Claim 47 is objected to because of the following informalities: the sixth limitation states "generating a second symmetrical encryption key based on the received random value." For the sake of examination the Examiner will interpret the limitation as "generating a second symmetrical encryption key based on the received random value;" (replacing the period with a semicolon). Appropriate correction is required.

Claim Rejections - 35 USC § 103

10. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 24, 25, 27-30, 33-35, 37, and 40-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 7,215,775 B2 to Noguchi et al., hereinafter Noguchi, in view of U.S. Patent Application Publication No. 2003/0033537 A1 to Fujimoto et al., hereinafter Fujimoto.

12. As per claims 24 and 40, Noguchi teaches a method and communication system for transmitting data, comprising:

by a first user of a communication network:

generating a first symmetrical encryption key based on the first random value (Figures 4, 10 [block 33], column 9, lines 41-50, column 12, lines 13-19);

a storage unit for storing the first symmetrical encryption key (Figure 10 [block 35], column 12, lines 22-25); and

transmitting the first random value to a second user of the communication network (Figures 4, 10 [block 31], column 9, lines 41-44, column 12, lines 17-22, i.e. sending a random number R and an ID that specifies an key generation algorithm to source A from destination B);

by the second user:

receiving the first random value from the first user (Figures 4, 10 [block 31], column 9, lines 51-56, i.e. source A uses random number R to generate symmetric key Kc); and

generating the first symmetrical encryption key based on the received random value (Figures 4, 10 [block 33], column 9, lines 51-56, i.e. source A uses random number R to generate symmetric key Kc).

13. Noguchi does not teach wherein the random value is generated from a stochastic process.

14. Fujimoto teaches generating a random number to a variation of voltage, timing, etc. and that this random number is used to generate a symmetric key (paragraphs 0050, 0056). According to paragraph 00013 of the specification, voltage is representative of a stochastic process.

15. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the random value be generated from a stochastic process, since Fujimoto states at paragraph 0051 that generating a random number in this manner for symmetric key generation makes it difficult to discover the random number externally thereby making it difficult for an eavesdropper to guess the key and decrypt the data.

16. Regarding claim 25, Fujimoto teaches wherein the first random value is an input to a function and an output of the function is used to generate the first symmetric encryption key (paragraphs 0050, 0056).

17. Regarding claim 27, Fujimoto teaches wherein the first random value is obtained by acquiring at least one measured value from the first stochastic process (paragraph 0050).

18. Regarding claim 28, Fujimoto teaches wherein the first stochastic process includes a time-variable parameter of an automation system (paragraph 0050).

19. Regarding claim 29, Fujimoto teaches wherein the first random value is a measured value (paragraph 0050).

20. Fujimoto and Noguchi do not disclose wherein the first user generates the first symmetrical encryption key based on the least significant bits of the first random value in order to at least reduce periodic components of the measure value; and wherein the second user generates the first symmetrical encryption key based on the least significant bits of the first random value in order to at least reduce periodic components of the measure value.

21. It would have been obvious to one of ordinary skill in the art at the time the invention was made to obtain the data from a least significant bit position of the measured data, since it is a well-known and common practice in art to read data from the least significant bit and merely amounts to a design choice.

22. Regarding claims 30 and 42, Noguchi teaches wherein data transferred between the users is encrypted and unencrypted via the symmetrical encryption keys (Figure 4 [cipher communication using the symmetric keys]).

23. Noguchi and Fujimoto do not disclose wherein the second user receives a second random value originating from a second stochastic process; generating a second symmetrical encryption key from a second stochastic process; transmitting the second random value to the first user; and the first user: receiving the second random value from the second user; and generating the second symmetrical encryption key based on the received random value.

24. It would have been obvious to one of ordinary skill in the art at the time the invention was made to duplicate the method of claims 24 and 40, respectively, for the second client, since it has been held that it only requires routine skill in the art to duplicate a method and that said duplication has no patentable significance unless new and unexpected results are produced. See MPEP § 2144.04; see *In re Harza*, 274 F.2d 669, 124 USPQ 378 (CCPA 1960).

25. With regards to claim 33, Noguchi and Fujimoto do not teach wherein the first and second symmetrical encryption keys are generated upon a request by a master user of the communication network.

26. It would have been obvious to one of ordinary skill in the art at the time the invention was made for one of the users to request the keys be generated, since the symmetric key generation had to be triggered by one of the two users in order to establish encrypted communications since the references do not disclose a third-party for initiating encrypted communications between the two parties.

27. With regards to claim 34, Fujimoto teaches wherein the first and second symmetrical encryption keys are generated at predetermined times or after a lapse of a predetermined time interval (paragraph 0050).

28. Regarding claim 35, Noguchi and Fujimoto do not teach wherein the first random value are transmitted over the communication network at a time of low utilization of the communication network.

29. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit data over the network at a time of low utilization, since one of ordinary skill in the art would realize that retrieving information about the communication channel when utilization was low would provide for better results without interference from any cross communication occurring on the network.

30. Regarding claim 37, Noguchi teaches wherein the first random value is transmitted using an asymmetrical encryption method (column 9, lines 20-50, i.e. destination B encrypts the random number R using the public key Kp received from source A).

31. Regarding claim 41, Noguchi teaches wherein the communication network is a public network (Figure 13 [elements 84, 92], column 13, lines 48-63).

32. With regards to claim 43, Noguchi teaches wherein the communication network is the Internet (Figure 13 [elements 84, 92], column 13, lines 48-63).

33. Noguchi and Fujimoto do not teach that the first user is a master user for triggering the generating of the first and second symmetrical encryption keys by issuing a request via the Internet.

34. It would have been obvious to one of ordinary skill in the art at the time the invention was made for one of the users to request the keys be generated, since the symmetric key generation had to be triggered by one of the two users in order to establish encrypted communications since the references do not disclose a third-party for initiating encrypted communications between the two parties.

35. With regards to claim 44, Noguchi and Fujimoto do not teach wherein the first or second user is a master user configured to output a command onto the Ethernet for triggering the generation of the first and second symmetrical encryption keys.

36. It would have been obvious to one of ordinary skill in the art at the time the invention was made for one of the users to request the keys be generated, since the symmetric key generation had to be triggered by one of the two users in order to establish encrypted communications since the references do not disclose a third-party for initiating encrypted communications between the two parties.

37. Regarding claim 45, Noguchi and Fujimoto do not teach wherein the first random value is transmitted to a plurality of users and the first symmetrical encryption key is generated at each of the plurality of users.

38. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the first user transmit the random value to a plurality of users, especially so since Noguchi includes identifying which algorithm to use to generate the key, since one of ordinary skill in the art would recognize the need for providing secure communications in a group type setting.

39. Claims 46-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Noguchi in view of Fujimoto as applied above, and further in view of U.S. Patent No. 6,973,499 B1 to Peden et al., hereinafter Peden.

40. With regards to claim 46, Noguchi and Fujimoto do not teach wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval.

41. Peden teaches wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval (column 6, lines 10-24, claim 18, i.e. a plurality of keys, wherein each key corresponds to one of a plurality of time intervals and each key being a symmetric key).

42. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the first symmetrical encryption key to be used to encrypt data transmitted during a first time interval and the second symmetrical encryption value to be used to encrypt data transmitted during a second time interval, since Peden states at column 2, lines 14-31 that

designating keys for certain time periods prevents unauthorized users from accessing data in an environment that has a constantly changing base of users.

43. As per claim 47, Noguchi teaches a method for transmitting data, comprising

by a first user of a communication network:

storing a first random measured value (Figure 10 [block 35], column 12, lines 22-25);

generating a first symmetrical encryption key based on the first random measured value (Figures 4, 10 [block 33], column 9, lines 41-50, column 12, lines 13-19);

transmitting the first measured random value to a second user of the communication network (Figures 4, 10 [block 31], column 9, lines 41-44, column 12, lines 17-22, i.e. sending a random number R and an ID that specifies an key generation algorithm to source A from destination B);

by the second user:

receiving the first random measured value from the first user (Figures 4, 10 [block 31], column 9, lines 51-56, i.e. source A uses random number R to generate symmetric key Kc);

generating the first symmetrical encryption key based on the received measured random value (Figures 4, 10 [block 33], column 9, lines 51-56, i.e. source A uses random number R to generate symmetric key Kc).

44. Noguchi does not teach wherein the random value is generated from a stochastic process.

45. Fujimoto teaches generating a random number to a variation of voltage, timing, etc. and that this random number is used to generate a symmetric key (paragraphs 0050, 0056).

According to paragraph 00013 of the specification, voltage is representative of a stochastic process.

46. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the random value be generated from a stochastic process, since Fujimoto states at paragraph 0051 that generating a random number in this manner for symmetric key generation makes it difficult to discover the random number externally thereby making it difficult for an eavesdropper to guess the key and decrypt the data.

47. Noguchi and Fujimoto do not disclose wherein the second user receives a second random value originating from a second stochastic process; generating a second symmetrical encryption key from a second stochastic process; transmitting the second random value to the first user; and the first user: receiving the second random value from the second user; and generating the second symmetrical encryption key based on the received random value and wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval.

48. It would have been obvious to one of ordinary skill in the art at the time the invention was made to duplicate the method generating the first client's symmetric key for the second client, since it has been held that it only requires routine skill in the art to duplicate a method and that said duplication has no patentable significance unless new and unexpected results are produced. See MPEP § 2144.04; see *In re Harza*, 274 F.2d 669, 124 USPQ 378 (CCPA 1960).

49. Peden teaches wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to

encrypt data transmitted during a second time interval (column 6, lines 10-24, claim 18, i.e. a plurality of keys, wherein each key corresponds to one of a plurality of time intervals and each key being a symmetric key).

50. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the first symmetrical encryption key to be used to encrypt data transmitted during a first time interval and the second symmetrical encryption value to be used to encrypt data transmitted during a second time interval, since Peden states at column 2, lines 14-31 that designating keys for certain time periods prevents unauthorized users from accessing data in an environment that has a constantly changing base of users.

51. Regarding claim 48, Fujimoto teaches wherein the first random value is an input to a function and an output of the function is used to generate the first symmetrical encryption key (paragraphs 0050, 0056).

52. Regarding claim 49, Fujimoto teaches wherein the second random value is an input to a function and an output of the function is used to generate the second symmetrical encryption key (paragraphs 0050, 0056).

Conclusion

53. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

54. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

55. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

56. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine L. Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

57. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

clf